PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-175008
(43)Date of publication of application : 21.06.2002

(51)Int.Cl. G09C 1/00

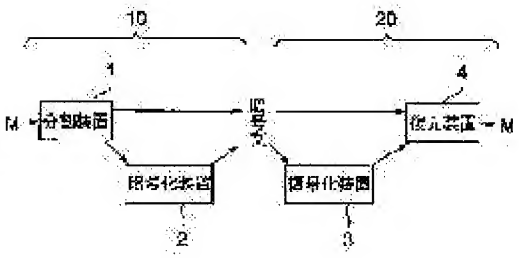
(21)Application number : 2001-291419
(22)Date of filing : 25.09.2001

(71)Applicant : NEC SOFT LTD
TSUJII SHIGEO
YDK:KK
MURATA MACH LTD
(72)Inventor : TSUJII SHIGEO
MATSUOKA KENJI

(30)Priority
Priority number : 2000294435 Priority date : 27.09.2000 Priority country : JP

(54) ENCRYPTION METHOD, ENCRYPTION UNIT, AND ENCRYPTION AND DECODING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an encryption and decoding system enabling configuration of a speedy and easy cryptographic system.
SOLUTION: This encryption and decoding system is provided with an encryption unit, which has a dividing device 1 for dividing a plain text M into r-pieces of divided plaintexts (r is an integer larger than one); an encryption device 2 for ciphering n-pieces of the divided plain texts among the r-prices of divided plain texts (n<r) into n-pieces of ciphertexts according to an arbitrary encryption method, and which outputs the remaining (r-n) pieces of divided plain texts and the n-pieces of ciphertexts as output ciphertexts; and a decoding unit 20 for receiving the output ciphertexts as in put ciphertexts, and the decoding unit 20 comprises a decoding device 3 for decoding the n-pieces of ciphertexts of the input ciphertexts into the n-pieces of divided plaintexts, and a restoring device 4 for restoring the plaintexts M from the remaining (r-n) pieces of divided plaintexts of the input ciphertexts and the n-pieces of divided plain texts from the decoding device 3.



LEGAL STATUS

[Date of request for examination] 25.09.2001
[Date of sending the examiner's decision of rejection] 25.05.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－175008
（P2002－175008A）
(43)公開日　平成14年６月21日(2002.6.21)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ｚ　５Ｊ１０４

審査請求　有　請求項の数11　ＯＬ　（全８頁）

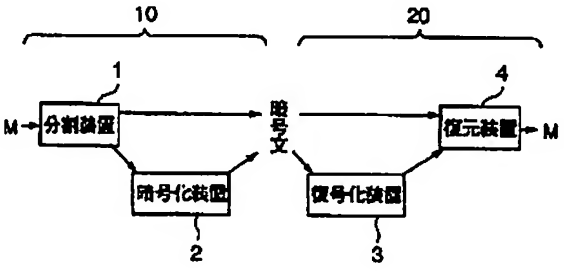
(21)出願番号　特願2001－291419(P2001－291419)
(22)出願日　平成13年９月25日(2001.9.25)
(31)優先権主張番号　特願2000－294435(P2000－294435)
(32)優先日　平成12年９月27日(2000.9.27)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000232092
エヌイーシーソフト株式会社
東京都江東区新木場一丁目18番６号
(71)出願人　598159964
辻井　重男
東京都渋谷区神宮前四丁目２番19号
(71)出願人　000139377
株式会社ワイ・デー・ケー
東京都稲城市押立1705番地
(74)代理人　100071272
弁理士　後藤　洋介　（外１名）

最終頁に続く

(54)【発明の名称】　暗号化方法、暗号化器、暗号化及び復号化システム

(57)【要約】
【課題】　高速で簡易な暗号系を構成できる暗号化及び復号化システムの提供。
【解決手段】　平文Ｍをｒ（ｒは２以上の整数）個の分割平文に分割する分割装置１と、ｒ個の分割平文のうちのｎ個（ｎ＜ｒ）の分割平文を、任意の暗号化方式によって、ｎ個の暗号文に暗号化する暗号化装置２とを有し、残りの（ｒ－ｎ）個の分割平文とｎ個の暗号文とを出力暗号文として出力する暗号化器１０と、出力暗号文を入力暗号文として受ける復号化器２０とを備えた暗号化及び復号化システムであって、復号化器２０は、入力暗号文のｎ個の暗号文をｎ個の分割平文に復号化する復号化装置３と、入力暗号文の残りの（ｒ－ｎ）個の分割平文と復号化装置３からのｎ個の分割平文とから、平文Ｍを復元する復元装置４とを有する。



1

【特許請求の範囲】

【請求項１】　平文Ｍをｒ（ｒは２以上の整数）個の分割平文に分割するステップと、ｒ個の分割平文のうちのｎ個（ｎ＜ｒ）の分割平文をｎ個の暗号文に暗号化するステップと、残りの（ｒ－ｎ）個の分割平文と前記ｎ個の暗号文とを出力暗号文として出力するステップとを含むことを特徴とする暗号化方法。

【請求項２】　平文Ｍをｒ（ｒは２以上の整数）個の分割平文に分割する分割装置と、ｒ個の分割平文のうちのｎ個（ｎ＜ｒ）の分割平文をｎ個の暗号文に暗号化する暗号化装置とを有し、残りの（ｒ－ｎ）個の分割平文と前記ｎ個の暗号文とを出力暗号文として出力することを特徴とする暗号化器。

【請求項３】　平文Ｍをｒ（ｒは２以上の整数）個の分割平文に分割する分割装置と、ｒ個の分割平文のうちのｎ個（ｎ＜ｒ）の分割平文を、任意の暗号化方式によって、ｎ個の暗号文に暗号化する暗号化装置とを有し、残りの（ｒ－ｎ）個の分割平文と前記ｎ個の暗号文とを出力暗号文として出力する暗号化器と；前記出力暗号文を入力暗号文として受ける復号化器と；を備えた暗号化及び復号化システムであって、

前記復号化器は、前記入力暗号文の前記ｎ個の暗号文を前記ｎ個の分割平文に復号化する復号化装置と、前記入力暗号文の前記残りの（ｒ－ｎ）個の分割平文と前記復号化装置からの前記ｎ個の分割平文とから、前記平文Ｍを復元する復元装置とを有することを特徴とする暗号化及び復号化システム。

【請求項４】　請求項３に記載の暗号化及び復号化システムにおいて、

前記分割装置は、ｒ個の分割平文をＣ1，Ｃ2，…，Ｃ(r-1)，Ｃｒとすると、どの２つをとってもお互いに公約数をもたないｒ個の自然数Ｎｉ　(i=1,2,…,r) を用いて、表わされる以下の式：

$C1 = M \bmod N_1$ ，

$C2 = M \bmod N_2$ ，

・・・，

$C(r-1) = M \bmod N_{r-1}$ ，

$Cr = M \bmod N_r$

に従って、平文Ｍをｒ個の分割平文Ｃ1，Ｃ2，…，Ｃ(r-1)，Ｃｒに分割することを特徴とする暗号化及び復号化システム。

【請求項５】　請求項４に記載の暗号化及び復号化システムにおいて、

前記ｒ個の自然数Ｎｉ　(i=1,2,…,r) の積Ｎを

$N = N_1 \cdot N_2 \cdot \cdots \cdot N_{r-1} \cdot N_r$

とした時、平分Ｍを$\log_2 M \leqq \log_2 N$を満たす整数とし、

Ｎｒを法とする、任意の公開鍵暗号方式の暗号化関数Ｅｒ( )を公開鍵とし、

暗号化関数Ｅｒ( )に対する復号化関数Ｄｒ( )を秘密鍵と

2

することを特徴とする暗号化及び復号化システム。

【請求項６】　請求項５に記載の暗号化及び復号化システムにおいて、

前記暗号化装置は、Ｂｒ＝Ｅｒ(Ｃｒ) によって、平分Ｍの一部であるＣｒをＢｒに暗号化し、

前記暗号化器は、Ｃ=(Ｃ1，Ｃ2，…，Ｃ(r-1)，Ｂｒ)を出力暗号文として出力することを特徴とする暗号化及び復号化システム。

【請求項７】　請求項６に記載の暗号化及び復号化システムにおいて、

前記復号化装置は、Ｃｒ=Ｄｒ(Ｂｒ)によりＣｒを求め、

前記復元装置は、

$C1 = M \bmod N_1$ ，

$C2 = M \bmod N_2$ ，

・・・，

$C(r-1) = M \bmod N_{r-1}$ ，

$Cr = M \bmod N_r$

から、前記平分Ｍを復元することを特徴とする暗号化及び復号化システム。

【請求項８】　請求項６に記載の暗号化及び復号化システムにおいて、

前記復号化装置は、Ｃｒ=Ｄｒ(Ｂｒ)によりＣｒを求め、

前記復元装置は、

$C1 = M \bmod N_1$ ，

$C2 = M \bmod N_2$ ，

・・・，

$C(r-1) = M \bmod N_{r-1}$ ，

$Cr = M \bmod N_r$

に中国人剰余定理(Chinese remainder theorem)を適用して、前記平分Ｍを復元することを特徴とする暗号化及び復号化システム。

【請求項９】　請求項３に記載の暗号化及び復号化システムにおいて、

前記分割装置は、平文Ｍをｒ個の平文Ｕ1，Ｕ2，…，Ｕｒに分割すると共に、Ｕ1，Ｕ2，…，Ｕｒをアダマール変換行列Ｈ(r,r)によって

Ｈ(r,r)・(Ｕ1，Ｕ2，…，Ｕｒ) = (Ｖ1，Ｖ2，…，Ｖｒ)

と表わされるＶ1，Ｖ2，…，Ｖｒに変換し、Ｖ1，Ｖ2，…，Ｖｒを前記ｒ個の分割平文として出力するものであることを特徴とする暗号化及び復号化システム。

【請求項１０】　請求項９に記載の暗号化及び復号化システムにおいて、

前記暗号化装置は、Ｖｒを法とする、任意の公開鍵暗号方式の暗号化関数Ｅｒ()を公開鍵とし、Ｂｒ＝Ｅｒ(Ｖｒ)によって、平分Ｍの一部であるＶｒをＢｒに暗号化し、

前記暗号化器は、Ｖ＝(Ｖ1，Ｖ2，…，Ｖ(r-1)，Ｂｒ)を出力暗号文として出力することを特徴とする暗号化及び復号化システム。

【請求項１１】　請求項１０に記載の暗号化及び復号化システムにおいて、

前記復号化装置は、暗号化関数Ｅｒ( )に対する復号化関数Ｄｒ( )を秘密鍵とし、Ｖｒ＝Ｄｒ(Ｂｒ)によりＶｒを求め、

前記復元装置は、Ｖ1,Ｖ2,…,Ｖ(r-1),Ｖｒを、アダマール変換行列Ｈ(r,r)の逆行列H^{-1}(r,r)によって、

H^{-1}(r,r)・(Ｖ1,Ｖ2,…,Ｖr)＝(Ｕ1,Ｕ2,…,Ｕr)

と表わされるＵ1,Ｕ2,…,Ｕrに変換して、前記平文Ｍを復元することを特徴とする暗号化及び復号化システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化方法、暗号化器、暗号化及び復号化システムに関し、特に公開鍵及び秘密鍵を用いて電子文書を暗号化及び復号化することにより、秘密通信を行う暗号化及び復号化システム（暗号情報変換装置）に関するものである。

【０００２】

【従来の技術】従来の暗号化方法は、送信者と受信者との間に、暗号文の復号に用いる暗号情報を変換する変換部を有するセンタを設けて、送信者は、受信者を示す受信者情報と、送信する情報を暗号化した暗号文と、この暗号文の復元に用いる第１の暗号情報とをセンタに送信し、センタは、送信者から受信者情報、暗号文および第１の暗号情報をそれぞれ受信し、変換部により第１の暗号情報を受信者情報の示す受信者が復元可能な第２の暗号情報に変換し、この第２の暗号情報と暗号文とを受信者に送信し、受信者は、センタから第２の暗号情報と暗号文とを受信し、第２の暗号情報に基づいて暗号文を復号化することにより元の情報を得るようにしたものである。

【０００３】さらに、暗号化及び復号化システム（暗号情報変換装置）は、自己の公開鍵を用いて暗号化された第１の暗号情報を入力する暗号情報入力部と、自己の秘密鍵を入力する装置秘密鍵入力部と、この自己の秘密鍵を用いて第１の暗号情報を復号化する復号部と、受信者の公開鍵を入力する受信者公開鍵入力部と、この受信者の公開鍵を用いて復号部からの出力を暗号化することにより第２の暗号情報を生成する暗号化部とを備えるものである。

【０００４】

【発明が解決しようとする課題】従来の技術の問題点は、実用化されている公開鍵暗号の方式は、暗号化・復号処理に要する計算量が、共通鍵暗号に比較して桁違いに大きく、その結果、公開鍵暗号の用途は、主にディジタル署名、または、鍵配送に限られていることである。

【０００５】それ故、本発明の目的は、高速で簡易な暗号系を構成できる暗号化方法、暗号化器、及び暗号化及び復号化システムを提供することにある。

【０００６】本発明のもう一つの目的は、任意の安全な公開鍵暗号を構成要素として含む、高速で簡易なメタ暗号系を、中国人剰余定理をベースに構成する方法を提案することである。

【０００７】本発明の別の目的は、任意の安全な公開鍵暗号を構成要素として含む、高速で簡易なメタ暗号系を、アダマール変換をベースに構成する方法を提案することである。

【０００８】

【課題を解決するための手段】本発明の第１の態様によれば、平文Ｍをｒ（ｒは２以上の整数）個の分割平文に分割するステップと、ｒ個の分割平文のうちのｎ個（ｎ＜ｒ）の分割平文をｎ個の暗号文に暗号化するステップと、残りの（ｒ－ｎ）個の分割平文と前記ｎ個の暗号文とを出力暗号文として出力するステップとを含むことを特徴とする暗号化方法が得られる。

【０００９】本発明の第２の態様によれば、平文Ｍをｒ（ｒは２以上の整数）個の分割平文に分割する分割装置と、ｒ個の分割平文のうちのｎ個（ｎ＜ｒ）の分割平文をｎ個の暗号文に暗号化する暗号化装置とを有し、残りの（ｒ－ｎ）個の分割平文と前記ｎ個の暗号文とを出力暗号文として出力することを特徴とする暗号化器が得られる。

【００１０】本発明の第３の態様によれば、平文Ｍをｒ（ｒは２以上の整数）個の分割平文に分割する分割装置と、ｒ個の分割平文のうちのｎ個（ｎ＜ｒ）の分割平文を、任意の暗号化方式によって、ｎ個の暗号文に暗号化する暗号化装置とを有し、残りの（ｒ－ｎ）個の分割平文と前記ｎ個の暗号文とを出力暗号文として出力する暗号化器と；前記出力暗号文を入力暗号文として受ける復号化器と；を備えた暗号化及び復号化システムであって、前記復号化器は、前記入力暗号文の前記ｎ個の暗号文を前記ｎ個の分割平文に復号化する復号化装置と、前記入力暗号文の前記残りの（ｒ－ｎ）個の分割平文と前記復号化装置からの前記ｎ個の分割平文とから、前記平文Ｍを復元する復元装置とを有することを特徴とする暗号化及び復号化システムが得られる。

【００１１】本発明の第４の態様によれば、前述の第３の態様による暗号化及び復号化システムにおいて、前記分割装置は、ｒ個の分割平文をＣ1,Ｃ2,…,Ｃ(r-1),Ｃｒとすると、どの２つをとってもお互いに公約数をもたないｒ個の自然数N_i（i=1,2,…,r）、すなわち、gcd(N_i,N_j)＝1がN_iとN_jとの最大公約数が１であることを表わすものとすると、gcd(N_i,N_j)＝1（i≠j，i，j=1,2,…,r）を満たすｒ個の自然数N_i（i=1,2,…,r）、を用いて、表わされる以下の式：

$C1 = M \bmod N_1$，

$C2 = M \bmod N_2$，

・・・，

$C(r-1) = M \bmod N_{r-1}$，

$Cr = M \bmod N_r$

に従って、平文Ｍをｒ個の分割平文Ｃ1,Ｃ2,…，Ｃ(r-1),Ｃｒに分割することを特徴とする暗号化及び復号化シ

ステムが得られる。

【００１２】本発明の第５の態様によれば、前述の第４の態様による暗号化及び復号化システムにおいて、前記ｒ個の自然数N_i (i=1,2,…,r) の積Nを

$N = N_1 \cdot N_2 \cdot \cdots \cdot N_{r-1} \cdot N_r$

とした時、平分Mを$\log_2 M \leqq \log_2 N$を満たす整数とし、Nrを法とする、任意の公開鍵暗号方式の暗号化関数Er( )を公開鍵とし、暗号化関数Er( )に対する復号化関数Dr( )を秘密鍵とすることを特徴とする暗号化及び復号化システムが得られる。

【００１３】本発明の第６の態様によれば、前述の第５の態様による暗号化及び復号化システムにおいて、前記暗号化装置は、Br = Er(Cr) によって、平分Mの一部であるＣｒをＢｒに暗号化し、前記暗号化器は、C=(C1,C2,…,C(r-1),Br)を出力暗号文として出力することを特徴とする暗号化及び復号化システムが得られる。

【００１４】本発明の第７の態様によれば、前述の第６の態様による暗号化及び復号化システムにおいて、前記復号化装置は、Cr=Dr(Br)によりＣｒを求め、前記復元装置は、

$C1 = M \bmod N_1$,
$C2 = M \bmod N_2$,
・・・,
$C(r-1) = M \bmod N_{r-1}$,
$Cr = M \bmod N_r$

から、前記平分Mを復元することを特徴とする暗号化及び復号化システムが得られる。

【００１５】本発明の第８の態様によれば、前述の第６の態様による暗号化及び復号化システムにおいて、前記復号化装置は、Cr=Dr(Br)によりＣｒを求め、前記復元装置は、

$C1 = M \bmod N_1$,
$C2 = M \bmod N_2$,
・・・,
$C(r-1) = M \bmod N_{r-1}$,
$Cr = M \bmod N_r$

に中国人剰余定理(Chinese remainder theorem)を適用して、前記平分Mを復元することを特徴とする暗号化及び復号化システムが得られる。

【００１６】本発明の第９の態様によれば、前述の第３の態様による暗号化及び復号化システムにおいて、前記分割装置は、平文Mをr個の平文U1, U2, …, Urに分割すると共に、U1, U2, …, Urをアダマール変換行列H(r,r)によって

$H(r,r) \cdot (U1,U2,\cdots,Ur) = (V1,V2,\cdots,Vr)$

と表わされるV1,V2,…,Vrに変換し、V1,V2,…,Vrを前記r個の分割平文として出力するものであることを特徴とする暗号化及び復号化システムが得られる。

【００１７】本発明の第１０の態様によれば、前述の第９の態様による暗号化及び復号化システムにおいて、前記暗号化装置は、Vrを法とする、任意の公開鍵暗号方式の暗号化関数Er()を公開鍵とし、Br = Er(Vr) によって、平分Mの一部であるＶｒをＢｒに暗号化し、前記暗号化器は、V = (V1,V2,…,V(r-1),Br)を出力暗号文として出力することを特徴とする暗号化及び復号化システムが得られる。

【００１８】本発明の第１１の態様によれば、前述の第１０の態様による暗号化及び復号化システムにおいて、前記復号化装置は、暗号化関数Er( )に対する復号化関数Dr( )を秘密鍵とし、Vr = Dr(Br)によりVrを求め、前記復元装置は、V1,V2,…,V(r-1),Vrを、アダマール変換行列H(r,r)の逆行列H^{-1} (r,r)によって、

$H^{-1}(r,r) \cdot (V1,V2,\cdots,Vr) = (U1,U2,\cdots,Ur)$

と表わされるU1,U2,…,Urに変換して、前記平文Mを復元することを特徴とする暗号化及び復号化システムが得られる。

【００１９】

【発明の実施の形態】次に本発明について詳細に説明する。

【００２０】本発明は、平分Mを、C1,C2,・・・,C(r-1),Cr とr個に分割し、Ｃｒだけは、任意の暗号化方式(暗号化関数Er( ))によって、Br = Er(Cr)と暗号化し、C=(C1,C2,・・・,C(r-1),Br)を暗号文とする。

【００２１】この時、CよりMが解読されることはない。

【００２２】また、Er( )に対する復号化関数Dr( )によって、Cr=Dr(Br)を求め、前記平分Mを復元する。

【００２３】暗号化関数Er( )を一方向性関数と仮定する。このとき、中国人の剰余定理（又はアダマール変換）により、(C1,C2,・・・.C(r-1),Br)よりMが得られることはない。

【００２４】従って、完全解読されることはないという意味で、本方式は安全であることが証明される。Mの情報の一部は、C1,C2,…,C(r-1)より、情報量的には、洩れていることになるが、具体的に平分の一部が明示的に解読されることはない。

【００２５】また、rを大きくする程、平分Mのビット当りの処置量は減少し高速になる。rは平分としての適正サイズ等を考慮して定められる。

【００２６】次に、本発明の実施例について図面を参照して説明する。

【００２７】図１を参照すると、本発明の第１の実施例による暗号化及び復号化システムは、暗号化器１０と、復号化器２０とを備えている。

【００２８】暗号化器１０は、平文Mをr（ｒは２以上の整数）個の分割平文に分割する分割装置１と、r個の分割平文のうちのｎ個（ｎ＜ｒ）の分割平文を、任意の暗号化方式によって、ｎ個の暗号文に暗号化する暗号化

装置2とを有し、残りの（r－n）個の分割平文と前記n個の暗号文とを出力暗号文として出力する。

【0029】復号化器20は、出力暗号文を入力暗号文として受ける。そして、復号化器20は、入力暗号文の前記n個の暗号文を前記n個の分割平文に復号化する復号化装置3と、前記入力暗号文の前記残りの（r－n）個の分割平文と前記復号化装置からの前記n個の分割平文とから、前記平文Mを復元する復元装置4とを有する。

【0030】以下、暗号化器10は、平分Mをr個に分割し、そのうちの一つを任意の暗号化方式によって暗号化装置2で暗号化するものとして説明する。

【0031】暗号化器10は、図2のように、分割装置1と、暗号化装置2とからなる。

【0032】分割装置1は、gcd（N_i，N_j）=1（$i \neq j$，i，j=1,2,…,r）を満たすr個の自然数N_i（i=1,2,…,r）の積$N = N_1 \cdot N_2 \cdot \cdots \cdot N_{r-1} \cdot N_r$に対して、平分Mを$\log_2 M \leqq \log_2 N$を満たす整数とし、

$C1 = M \bmod N_1$，
$C2 = M \bmod N_2$，
・・・，
$C(r-1) = M \bmod N_{r-1}$，
$Cr = M \bmod N_r$

のように平分Mをr個に分割する。

【0033】ただし、gcd（N_i，N_j）=1は、N_iとN_jとの最大公約数が1であることを意味する。なお、gcdはGreatest Common Divisorの略である。

【0034】すなわち、gcd（N_i，N_j）=1（$i \neq j$，i，j=1,2,…,r）を満たすr個の自然数N_i（i=1,2,…,r）とは、どの2つをとってもお互いに公約数をもたないr個の自然数N_i（i=1,2,…,r）ともいうことができる。

【0035】暗号化装置2は、Nrを法とする、任意の公開鍵暗号方式の暗号化関数Er( )を公開鍵とし、Br = Er(Cr) によって、平分Mの一部であるCrをBrに暗号化する。

【0036】最終的に、暗号化器10は、C=(C1,C2,・・・,C(r-1),Br)を、暗号文として出力する。

【0037】復号化器20は、図3のように、復号化装置3と、復元装置4とからなる。

【0038】復号化装置3は、暗号化関数Er( )に対する復号化関数Dr( )を秘密鍵として、Cr=Dr(Br)によりCrを復号化する。

【0039】復元装置4は、

$C1 = M \bmod N_1$，
＊$C2 = M \bmod N_2$，
・・・，
$C(r-1) = M \bmod N_{r-1}$，
$Cr = M \bmod N_r$

に中国人剰余定理(Chinese remainder theorem)を適用して、平分Mを復元する。中国人剰余定理は、中国では、孫子の剰余定理とも呼ばれている。中国人剰余定理を用いれば、$C1 = M \bmod N_1$，$C2 = M \bmod N_2$，・・・，$Cr = M \bmod N_r$からMが一意に決まる。

【0040】次に、上述の第1の実施例の動作を説明する。

【0041】具体例として、r = 3の場合において、M=1024 を分割、暗号化し、復号化、復元する場合を説明する。

【0042】$N_1 = 7, N_2 = 11, N_3 = 15 (= 3*5)$
$N = 7*11*15 = 1155$
M = 1024 とする。

【0043】
$C1 = M \bmod N_1$
$= 1024 \bmod 7 = 2 \bmod 7$
$C2 = M \bmod N_2$
$= 1024 \bmod 11 = 1 \bmod 11$
$C3 = M \bmod N_3$
$= 1024 \bmod 15 = 4 \bmod 15$
C3は任意の公開鍵暗号方式で暗号化する。

【0044】B3 = E3(C3)
C = (C1, C2, B3) を暗号文として送る。

【0045】B3 を C3 に復号化する。

【0046】C3 = D3(B3)
$C1 = 2 \bmod 7$
$C2 = 1 \bmod 11$
$C3 = 4 \bmod 15$
より中国人剰余定理を用いて M=1024 を復元する。

【0047】以下、中国人剰余定理の部分を説明する。

【0048】$ni = N/N_i$
ここでは
$n1 = N/N_1$
$= 1155/7 = 165$
$n2 = N/N_2$
$= 1155/11 = 105$
$n3 = N/N_3$
$= 1155/15 = 77$
$ni*xi = 1 \bmod N_i$
ここでは
x1 = 2,x2 = 2,x3 = 8

$$M = C1*n1*x1 + C2*n2*x2 + \cdots + Cr*nr*xr \pmod N$$
$$= 2*165*2 + 1*105*2 + 4*77*8 \pmod{1155}$$
$$= 3334 \pmod{1155}$$
$$= 1024 \pmod{1155}$$

より M = 1024 を得る。

【００４９】次に、本発明の第２の実施例による暗号化及び復号化システムについて説明する。

【００５０】この暗号化及び復号化システムは、図４に示した暗号化器１０'と、図５に示した復号化器２０'とを備えている。

【００５１】図４において、暗号化器１０'は、平文Mをr（rは２以上の整数）個の分割平文に分割する分割装置１'と、r個の分割平文のうちのｎ個（ｎ＜ｒ）の分割平文を、任意の暗号化方式によって、ｎ個の暗号文に暗号化する暗号化装置２'とを有し、残りの（ｒ－ｎ）個の分割平文と前記ｎ個の暗号文とを出力暗号文として出力する。

【００５２】図５において、復号化器２０'は、出力暗号文を入力暗号文として受ける。そして、復号化器２０'は、入力暗号文の前記ｎ個の暗号文を前記ｎ個の分割平文に復号化する復号化装置３'と、前記入力暗号文の前記残りの（ｒ－ｎ）個の分割平文と前記復号化装置からの前記ｎ個の分割平文とから、前記平文Mを復元する復元装置４'とを有する。

【００５３】以下、暗号化器１０'は、平分Mをr個に分割し、そのうちの一つを任意の暗号化方式によって暗号化装置２'で暗号化するものとして説明する。

【００５４】図４において、暗号化器１０'は、分割装置１'と、暗号化装置２'とからなる。

【００５５】分割装置１'は、平文Mを、ｒ個の平文U1, U2, …, Urに分割すると共に、U1, U2, …, Urをアダマール変換行列H(r,r)によって

H(r,r)・(U1,U2,…,Ur) = (V1,V2,…,Vr)

と表わされるV1,V2,…,Vrに変換し、V1,V2,…,Vrをr個の分割平文として出力する。

【００５６】暗号化装置２'は、Vrを法とする、任意の公開鍵暗号方式の暗号化関数Ｅr()を公開鍵とし、Ｂr = Ｅr(Vr) によって、平分Mの一部であるＶｒを暗号化する。

【００５７】最終的に、暗号化器１０'は、V=(V1,V2,…,V(r-1),Br)を、出力暗号文として出力する。

【００５８】図５において、復号化装置３'は、暗号化関数Ｅr( )に対する復号化関数Ｄr()を秘密鍵として、Vr=Dr(Br)によりVrを求める。

＊【００５９】復元装置４'は、V1,V2,…,V(r-1),Vrを、アダマール変換行列H(r,r)の逆行列H^{-1} (r,r)によって、

H^{-1} (r,r)・(V1,V2,…,Vr) = (U1,U2,…,Ur)

と表わされるU1,U2,…,Urに変換して、前記平文Mを復元する。

【００６０】次に、上述の第２の実施例の動作を説明する。

【００６１】具体例を、r = 4として、M=1234を分割、暗号化し、復号化、復元する。

【００６２】U1=1,U2=2,U3=3,U4=4と分割する。

【００６３】アダマール変換行列H(r,r)によって、

H(r,r)・(U1,U2,U3,U4) = (V1,V2,V3,V4)

と変換する。

【００６４】r = 4であるから、アダマール変換行列H(r,r)は

H(4,4)=((1, 1, 1, 1),(1,-1, 1,-1),(1, 1,-1,-1),(1,-1,-1, 1))

である。

【００６５】

H(r,r)・(U1,U2,U3,U4)=H(4,4)・(1,2,3,4)
=(10,-2, 0,-4)
=(V1,V2,V3,V4)

V4=-4は任意の公開鍵暗号方式で暗号化する。

【００６６】B4 = E4(-4)

V = (V1,V2,V3,B4)

= (10,-2, 0,B4)を暗号文として送る。

【００６７】B4をV4に復号化する。

【００６８】

V4 = D4(B4)

= -4

アダマール変換行列H(4,4)の逆行列H^{-1} (4,4)によって、

H^{-1} (4,4)・(V1,V2,V3,V4)=(U1,U2,U3,U4)

と変換する。

【００６９】r=4であるから、逆行列H^{-1} (4,4)は

H^{-1} (4,4)=(1/4)((1, 1, 1, 1),(1,-1, 1,-1),(1, 1,-1,-1),(1,-1,-1, 1))である。

【００７０】

H^{-1} (r,r)・(V1,V2,V3,V4)=H^{-1} (4,4)・(10,-2, 0,-4)
=(1, 2, 3, 4)
=(U1,U2,U3,U4)

より、M=1234を得る。

【００７１】

【発明の効果】以上説明したように、本発明による第１の効果は、安全性である。

【００７２】平分Mは、Ｎr（又はＶｒ）だけの不確定さで、復号者以外に秘匿される。

【００７３】また、実際には、Ｅr( )の完全な一方向性は保証されないので、例えば、RSA(Rivest-Shamir-Adleman)暗号と楕円エルガマル暗号等、２種類以上の公開鍵暗号方式を、複雑さと処理速度とのトレードオフを考慮しつつ、併用することも考えられる。

【００７４】本発明による第２の効果は、高速性である。

【００７５】r=10とすると、暗号化・復号処理速度は１

０倍近く向上するものと期待される。

【図面の簡単な説明】

【図１】本発明の第１の実施例による暗号化及び復号化システムのブロック図である。

【図２】図１の暗号化及び復号化システムにおける暗号化器１０のブロック図である。

【図３】図１の暗号化及び復号化システムにおける復号化器２０のブロック図である。

【図４】本発明の第２の実施例による暗号化及び復号化システムのおける暗号化器１０’のブロック図である。

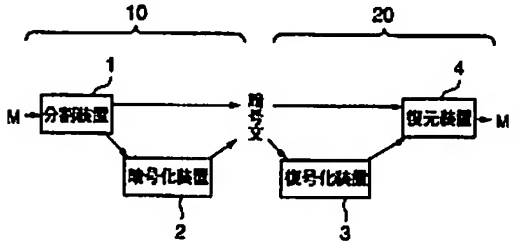
【図５】前述の第２の実施例による暗号化及び復号化システムのおける復号化器２０’のブロック図である。

【符号の説明】

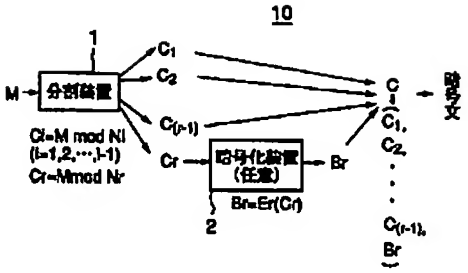
＊

＊１　分割装置
２　暗号化装置
３　復号化装置
４　復元装置
１０　暗号化器
２０　復号化器
１’　分割装置
２’　暗号化装置
３’　復号化装置
４’　復元装置
１０’　暗号化器
２０’　復号化器

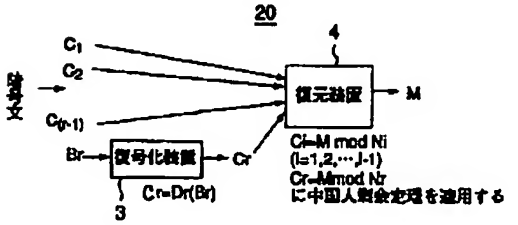
【図１】



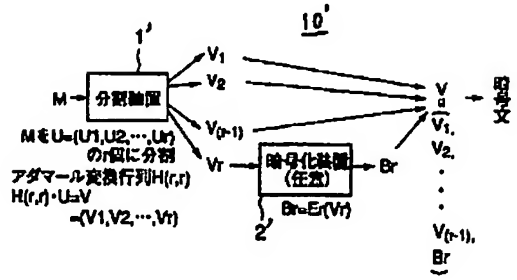
【図２】



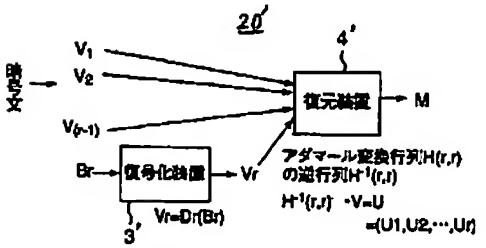
【図３】



【図４】



【図５】



フロントページの続き

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地
(72)発明者　辻井　重男
東京都渋谷区神宮前四丁目２番19号
(72)発明者　松岡　賢志
東京都江東区新木場一丁目18番６号　エヌイーシーソフト株式会社内
Ｆターム(参考)　5J104 AA18 JA26 NA02